



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,174	05/10/2001	Johan Cornelis Talstra	NL000262	5915
24737	7590	08/01/2005		
PHILIPS INTELLECTUAL PROPERTY & STANDARDS P.O. BOX 3001 BRIARCLIFF MANOR, NY 10510				
			EXAMINER POLTORAK, PIOTR	
			ART UNIT 2134	PAPER NUMBER

DATE MAILED: 08/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/853,174

Applicant(s)

TALSTRA ET AL.

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 May 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. The Amendment, and remarks therein, received on 5/13/2005 have been entered and carefully considered.
2. The Amendment introduces amends claims 1, 4, 8-9, 11, 13 16-17 and 19-20
3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

4. Applicant's arguments have been carefully considered but they were not found persuasive.
5. The applicant states that "The Office Actions employs Official Notice nine (9) times".
6. The statement is not understood. The examiner found only 7 Official Notice citations, one of which is included in the section Title 35, U.S. Code. As a result, unless clearly pointed out the location of the remaining two "Official Notices" the examiner addresses only six Official Notices rejections used in the previous Office Action.
7. As per claims 1, 3, 13-14, 16-17 and 19 applicant argues that the limitation "if a second signal but no physical mark is detected" is not taught by *Bloom et al.*
8. Applicant's argument is not found persuasive. *Bloom et al.* teach that "only if the additional watermark payload and transformed wobble bits match is playback allowed (pg. 1275 § 2)". A disk with no physical mark (*wobble*) does not have physical mark bits and as a result, it is anticipated that in such a disk there is no

match between the additional watermark payload and transformed physical mark bits, thus no playback is allowed.

9. Applicant argues that "the second signal containing a single bit trigger" is not disclosed by *Wirtz*.
10. The examiner points out that this limitation is a newly introduced limitation into the independent claims 1, 3, 13-14, 16-17 and 19, and as a result this limitation is addressed in this Office Action, below.
11. In regard to the claims 1, 3, 13-14, 16-17 and 19 rejection over *Glogau et al.* in view of *Bloom et al.* and *Wirtz* applicant argues that "there is no prima facie case of obviousness made by this rejection".
12. Applicant's argument is not found persuasive. The examiner points applicant to § 25-26 in the previous Office Action.
13. As per claim 8 applicant argues that neither *Wirtz* nor *Bloom et al.* teach the second signal that is logically contained within the first signal within encrypted packets, and that there is no prima facie case of obviousness made by this rejection.
14. Applicant's argument is not found persuasive. The examiner points out that claim 8 has been rejected by 35 U.S.C. 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter. The rejection of claim 8 (§ 28) precedes the statement: "Claim 8 is treated as best understood".

However, applicant chose to only point out why the rejection did not read on the claim language. Specifically, applicant provides an argument that neither *Wirtz* nor *Bloom et al.* teach "the second signal is logically contained within the first signal

within encrypted packets", and states that there is no prima facie case of obviousness.

The examiner points out that the limitation in question relates to claim 5. However, in order to address applicant's arguments the examiner points to the previous Office Action (§ 28-30).

15. Furthermore, the examiner points out that applicant added a minor amendment to claim 8 but chose not to elaborate on the intended meaning of the limitation (in light of the claim limitations, which claim 8 incorporates by virtue of its dependence). As a result, claim 8 remains rejected by 35 U.S.C. 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter. For purposes of further examination the examiner chose an interpretation, but appropriate explanation should be provided if other more appropriate interpretation is required.
16. As per claims 2, 4, 15 and 18 applicant traverses the Official Notice rejections used by the examiner.
17. As per claim 4 applicant contest that it is old and well-known practice to represent the decision with using a single bit to trigger appropriate action.
18. The examiner provides the *Lysakowski, Jr.* reference, wherein one bit is used to detect certain ... that triggers appropriate action (*allow or disallow modification, U.S. Patent No. 5434971, col. 6 lines 46-52*) and the *Newman et al.* (*U.S. Patent No. 5897671*) reference, which provides even more explicit information regarding the

subject (*Newman et al.*, col. 6 lines 31-63). Thus the traversal of Official Notice is not convincing.

19. As per claims 2, 15 and 18, despite the applicant's lack of knowledge that it is old and well-known practice to use a CD disk as the information carrier the examiner provides *Microsoft Press* that teach that a CD-ROM is a form of storage capable of storing data (pg. 82). In order to avoid any confusion, the examiner points to pg. 81 that clarifies that CD-ROM is an acronym for compact disk (CD). Thus the traversal of Official Notice is not convincing.
20. As per claim 9, despite the applicant's lack of knowledge that it is old and well-known practice to protect data signals by encrypting the data signals using encryption keys the examiner provides the *Microsoft's* definition of encryption, that defines "encryption" as a process of encoding data to prevent unauthorized access based on a key that is essential for encoding (*Microsoft*, pg. 175). Although *Microsoft* provides only one encryption scheme on pg. 175 (*DES*), the examiner refers to any security book containing basic information on cryptography (e.g. *Bruce Schneier*, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457) that deals with cryptography. In particular there at least two groups of keys, and using DES for an encryption is nothing less than a key selection from a symmetric (and not an asymmetric group) (*Stallings*, *Conventional Encryption: Modern Techniques*, pg. 49). Thus the traversal of Official Notice is not convincing.

21. The obviousness statements that correspond to Official Notices can be found in the previous and the current Office Actions.
22. Claims 1-20 have been examined.

Oath/Declaration

23. The oath or declaration is defective. A new oath or declaration signed and dated in compliance with 37 CFR § 1.66 or § 1.68 is required

Specification

24. The abstract of the disclosure is objected to because the phrase: "Embodiment propose" is missing an article and either "Embodiment" or "propose" is missing a letter "s". Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

25. Claim 4 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.
26. Claim 4 has been amended to include "the second signal is embedded in the first signal as a key". In applicant's remarks, applicant states that applicant does not

believe there was the introduction of new matter into the present application for invention. Applicant did not offer any support for the newly introduced limitation.

However, in the specification the examiner found citations that contradict the newly amended claim 4 language. For example, the last paragraph on page 5 reads: *"the second signal is embedded in the first signal by selecting a key"*, or the last paragraph on page 11 recites: *"a second signal hidden in an encrypted stream (first signal) is by using the freedom in the choice of the encryption key"*.

For purposes of further examination the examiner assumes that applicant mistakenly placed the word "as" instead of "with".

27. The phrase: "logically embedded" as cited in reference to the second signal (*claims 1, 13-14 and 16-17*) is not understood.

28. Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.

29. The meaning of claim 8 remains not understood. For details see *"Response to Amendment"* section, above.

30. Claims 1-20 are rejected under 35 U.S.C. 103 (a) as being unpatentable over *Glogau et al. (International Pub. No. WO 99/11020)* in view of *Bloom et al. (Bloom, J.A.; Cox, I.J.; Kalker, T.; Linnartz, J.-P.M.G.; Miller, M.L.; Traw, "Copy protection for DVD video", C.B.S.Proceedings of the IEEE , Volume: 87 , Issue: 7 , July 1999 Pages:1267 - 1276)* and *Wirtz (U.S. Patent No. 5940134)*.

Art Unit: 2134

31. As per claim 17 *Glogau et al.* teach a second signal (*secret message*) embedded in the first signal (*digital image (or digital audio pg. 4 lines 31-32)) (Glogau et al. pg. 5 lines 1-20 and Fig. 2).*
32. *Glogau et al.* do not teach the first signal/physical mark in which a second signal is logically embedded, and which could be used for refusing playback of the information read from the information carrier if a second signal but no physical mark were detected.
33. *Bloom et al.* teach the first signal/physical mark in which a second signal is logically embedded, and which could be used for refusing play back of the information read from the information carrier if a second signal but no physical mark were detected (*Bloom et al., pg. 1275 § 2*). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the first signal/physical mark in which a second signal is logically embedded, and which could be used for refusing play back of the information read from the information carrier if a second signal but no physical mark were detected as taught by *Bloom et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to provide a way to distinguish ROM disks from recordable and rewritable disks (*Bloom et al., pg. 1275 § 2*).
34. *Wirtz* teaches the first signal/physical mark in which a second signal is logically embedded, and which could be used for refusing play back of the information read from the information carrier if a second signal but no physical mark were detected (*Wirtz col. 2 lines 34-48 and col. 3 lines 42-47*). It would have been obvious to one

of ordinary skill in the art at the time of applicant's invention to incorporate the first signal/physical mark in which a second signal is logically embedded, and which could be used for refusing play back of the information read from the information carrier if a second signal but no physical mark were detected as taught by *Wirtz*.

One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent the reproduction of the disk copy (*Wirtz, col. 2 lines 40-48*).

35. *Glogau et al.* in view of *Bloom et al.* and *Wirtz* does not explicitly teach the second signal containing a single bit trigger.

36. Official Notice is taken that it is old and well-known practice to represent the decision with using a single bit to trigger appropriate action ("copy?" Y/N or "look for wobble?" Y/N, e.g. *Lysakowski, Jr., col. 6 lines 46-52*). One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ a single bit to take advantage of simplicity and speed while making decisions as to whether a desired action should be triggered.

37. Claims 1, 3, 14, 16 and 19-20 are substantially equivalent to claim 17; therefore claims 1, 3, 14, 16 and 19-20 are similarly rejected.

38. As per claims 5-8 *Glogau et al.* teach the second signal being embedded in the first signal by encoding it in a pseudo-random noise pattern of encrypted and unencrypted packs of the first signal, wherein the encryption sequence generated is based on a linear feedback shift register (*pg. 2 lines 14-17*).

Art Unit: 2134

39. *Glogau et al.* in view of *Bloom et al.* and *Wirtz* do not explicitly teach the linear feedback shift register (*LFSR*) being over Galois Field. However, pseudo-random numbers generate 1s and 0s, which appear fairly random, but after certain times the numbers repeat, and for the purposes of security the interest is to extend the time of this repeat to as long as possible. The choice of a minimal and irreducible polynomial function (*such as Galois*) which gives a long time period without the repeat would have been obvious to one of ordinary skill in the art given that they are well known and barring any unexpected results.
40. Also, in the XOR function 1s are ignored and 0s influence the result, which reads on "and its output is biased by interpreting emitted symbols '0'...'s-n-1' as 'unencrypted and 's-n'...'s-1' as 'encrypted'.
41. As per claims 2, 15 and 18 *Bloom et al.* teach the information carrier being DVD. However, neither *Glogau et al.* nor *Bloom et al.* and *Wirtz* explicitly teach the information carrier to be CD. Official notice is taken that it is old and well-known practice to use CD disc as the information carrier (e.g. *Microsoft, CD-ROM pg. 81-82*). One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ a CD disc as the information carrier given the benefit of an inexpensive portable large storage space.
42. Also, as per claim 4 *Glogau et al.* in view of *Bloom et al.* and *Wirtz* do not teach (a single bit trigger) within a message containing encrypted and unencrypted packs.
43. Official Notice is taken that it is old and well-known practice to implement a single bit trigger (e.g. *Lysakowski, Jr., U.S. Patent No. 5434971, col. 6 lines 46-52 and*

Art Unit: 2134

Newman et al., col. 6 lines 31-63). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement a single bit trigger.

One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ a single bit trigger in order to include additional security information associated with permitted/prohibited activities (e.g. *modify/copy Y/N*).

44. Placing the single bit trigger within a message containing encrypted and unencrypted packs would have been obvious to one of ordinary skill in the art at the time of applicant's invention for motivation of benefit of minimizing the chances to identify and alter the single bit trigger.

45. As per claim 9 *Blook et al.* teach that an encryption such as PGP or RSA can be used to at least partly encrypt the information (*Blook et al.*, pg. 5 lines 5-6).

46. *Glogau et al.* in view of *Bloom et al.* and *Wirtz* do not explicitly teach selecting the key from one of at least two groups of keys.

47. Official Notice is taken that it is old and well-known practice to have more than one key available in a system (e.g. *Taguchi et al.*, U.S. Patent No. 5915025 teach multiple groups with multiple keys, col. 23 lines 16-29 and Fig. 25). One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ more than one key in order to provide more flexibility and compatibility for encryption using systems. In the multiple key systems selecting a key from one of at least two groups of keys is implicit.

48. Claim 10 is implicit since the purpose of encryption is to ensure data security, wherein the data is to be later decrypted.

Art Unit: 2134

49. As per claim 11 computers project all information to n-bit numbers (0s and 1s) to accommodate a particular processor used in the computers.

50. As per claim 12 *Glogau et al.* in view of *Bloom et al.* and *Wirtz* do not explicitly teach that said examining process takes the form of going down a binary tree, where said going left is caused by projection-value 0 and right by projection in value non-zero. However, Official Notice is taken that it is old and well-known practice to use a binary search, which is one of the most fundamental search techniques (e.g. *Robert Sedgewick, "Algorithms", second edition, 1998, ISBN: 0201066734, pg. 198*) for motivation of benefit of an efficient searching. Also, in a binary tree going one direction is caused by one projection value and another direction is caused by another projection value. Thus, having an option of selecting 01/ or 1/0 for moving left/right or right/left the binary tree is simply inherent.

51. Also, as per claim 13 *Glogau et al.* in view of *Bloom et al.* and *Wirtz* do not teach that the second signal contains an encrypted trigger.

52. Official Notice is taken that it is old and well-known practice to implement a trigger (e.g. *Lysakowski, Jr., U.S. Patent No. 5434971, col. 6 lines 46-52 and Newman et al., col. 6 lines 31-63*). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement a trigger. One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ a single bit trigger in order to include additional security information associated with permitted/prohibited activities (e.g. *modify/copy Y/N*).

53. Also, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to encrypt the trigger. Since the trigger is one of the mechanisms that implements a systems' security, one of ordinary skill in the art would have been motivated to encrypt the trigger in order to make it more difficult to circumvent the system's security.

Conclusion


Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866) 217-9197 (toll-free).


Signature
7/14/05
Date

David Y. Jung
Primary Examiner

David Y. Jung
Primary Examiner

D.Y. Jung
7/21/05